

1/5/1 (Item 1 from file: 351)  
DIALOG(R) File 351: Derwent WPI  
(c) 2002 Thomson Derwent. All rts. reserv.

011113820 \*\*Image available\*\*  
WPI Acc No: 1997-091745/ 199709  
XRPX Acc No: N97-075652

Computer network system for e.g. security processing, access management -  
uses data transceiver of each connected data processor in sending and  
receiving formed description data as user identifier through  
communication network

Patent Assignee: TOSHIBA KK (TOKE )  
Inventor: ITSUMI K; NUKUI H; UCHIDA S  
Number of Countries: 002 Number of Patents: 002  
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 8329010	A	19961213	JP 9659806	A	19960315	199709 B
US 5887140	A	19990323	US 96622608	A	19960326	199919

Priority Applications (No Type Date): JP 9568185 A 19950327

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 8329010	A	23	G06F-015/00	
US 5887140	A		G06K-009/00	

Abstract (Basic): JP 8329010 A

The system (10) has several data processors (11-1-11-3) connected  
through a communication network (12). Each data processor has a  
measuring unit that measures the physical description of a user.

A data generator forms a description data based on the measured  
physical description. A data transceiver sends and receives the formed  
description data as a user identifier through the communication  
network.

ADVANTAGE - Reliably maintains security. Determines access right  
based on access demand of user at high speed. Reduces user load since  
reliable authentication processing is performed through easy operation.  
Eliminates complex password input operation in access processing.  
Ensures high-speed collation processing. Increases capacity of file  
system ten times higher than conventional system.

Dwg.1/15

Title Terms: COMPUTER; NETWORK; SYSTEM; SECURE; PROCESS; ACCESS; MANAGEMENT  
; DATA; TRANSCEIVER; CONNECT; DATA; PROCESSOR; SEND; RECEIVE; FORMING;  
DESCRIBE; DATA; USER; IDENTIFY; THROUGH; COMMUNICATE; NETWORK

Derwent Class: T01

International Patent Class (Main): G06F-015/00; G06K-009/00

International Patent Class (Additional): G06F-013/00; G06T-007/00

File Segment: EPI

1/5/2 (Item 1 from file: 347)  
DIALOG(R) File 347: JAPIO  
(c) 2002 JPO & JAPIO. All rts. reserv.

05373510 \*\*Image available\*\*  
COMPUTER NETWORK SYSTEM, ITS ACCESS ADMINISTRATING METHOD, AND INDIVIDUAL  
AUTHORIZATION DEVICE USED FOR SAME

PUB. NO.: 08-329010 [ JP 8329010 A]  
PUBLISHED: December 13, 1996 (19961213)  
INVENTOR(s): HENMI KAZUHIRO  
UCHIDA SATOSHI  
NUKUI HARUMI

APPLICANT(s): TOSHIBA CORP [000307] (A Japanese Company or Corporation), JP  
(Japan)

APPL. NO.: 08-059806 [JP 9659806]  
FILED: March 15, 1996 (19960315)

INTL CLASS: [6] G06F-015/00; G06F-013/00; G06T-007/00  
JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 45.2  
(INFORMATION PROCESSING -- Memory Units); 45.9 (INFORMATION  
PROCESSING -- Other)  
JAPIO KEYWORD: R124 (CHEMISTRY -- Epoxy Resins)

#### ABSTRACT

PURPOSE: To perform a processing for deciding whether or not a user has access right speedily at a user's access request by using physical body feature data and to securely maintain secrecy protection.

CONSTITUTION: At the access request, the physical body features of the user are measured by feature measurement units 14-1, 14-2, and 14-3, and further processed by data degeneration units 13-1, 13-2, and 13-3 as feature data having linear projection, etc., degenerated. Computer systems 11-1 and 11-2 send the feature data to a collation server 15 through a communication network 12. The collation server 15 performs a collation process according to feature data previously stored in a file system 16. It is judged from the collation result whether or not the user has the access right, and the access allowed/disallowed state is sent to computer systems 11-1 and 11-2.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-329010

(43) 公開日 平成8年(1996)12月13日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0	9364-5L	G 0 6 F 15/00	3 3 0 F
13/00	3 5 5	7368-5E	13/00	3 5 5
G 0 6 T 7/00			15/62	4 6 0

審査請求 未請求 請求項の数14 O L (全 23 頁)

(21) 出願番号 特願平8-59806

(22) 出願日 平成8年(1996)3月15日

(31) 優先権主張番号 特願平7-68185

(32) 優先日 平7(1995)3月27日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 逸見 和弘

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 内田 智

神奈川県川崎市幸区柳町70番地 株式会社東芝柳町工場内

(72) 発明者 貫井 春美

東京都府中市東芝町1番地 株式会社東芝府中工場内

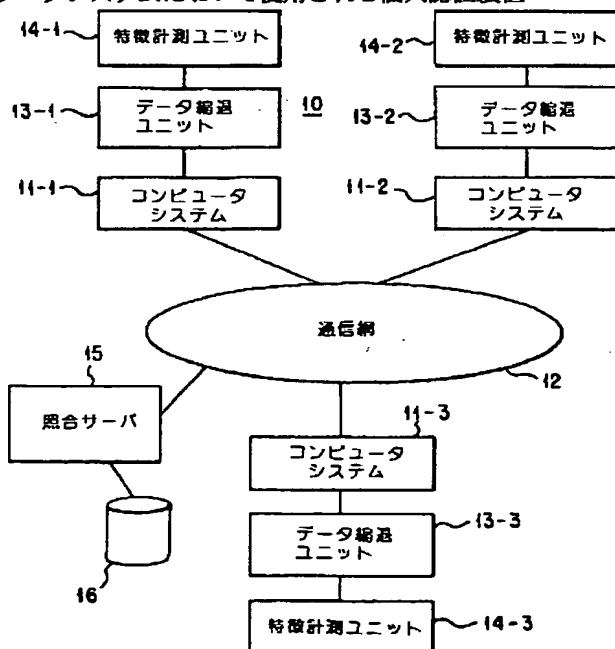
(74) 代理人 弁理士 鈴江 武彦

(54) 【発明の名称】 コンピュータネットワークシステム、このコンピュータネットワークシステムにおけるアクセス管理方法、及びこのコンピュータネットワークシステムにおいて使用される個人認証装置

(57) 【要約】

【課題】 コンピュータネットワークシステムにおいて、身体的特徴データを用い、使用者からのアクセス要求に応じてアクセス権の有無を判別する処理を高速に行い、且つ、確実に機密保護を維持する。

【解決手段】 アクセス要求に応じ、使用者の身体的特徴が特徴計測ユニット14により計測され、更に、データ縮退ユニット13において、一次元射影等の縮退された特徴データとして処理される。コンピュータシステム11は、通信網12を介してこの特徴データを照合サーバ15に送出する。照合サーバ15は、ファイルシステム16に予め登録されている特徴データに従って照合処理を行う。この照合結果に応じて、使用者のアクセス権の有無が判断され、アクセス許可／不許可の旨がコンピュータシステム11に送られる。



## 【特許請求の範囲】

【請求項1】 複数のデータ処理手段と前記複数のデータ処理手段を相互接続する通信手段とにより構成されるコンピュータネットワークシステムにおいて、前記複数のデータ処理手段はそれぞれ、使用者の身体的特徴を測定する測定手段と、測定された身体的特徴を縮退して特徴データを生成する生成手段と、前記特徴データを使用者識別子として前記通信手段を介して送受するデータ送受手段とを具備することを特徴とするコンピュータネットワークシステム。

【請求項2】 前記複数のデータ処理手段は、アクセス要求に応じて前記使用者識別子を送出し、前記通信手段に接続され、前記通信手段を介して受け取った使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する照合手段を具備することを特徴とする請求項1記載のコンピュータネットワークシステム。

【請求項3】 前記コンピュータネットワークシステムは、任意のデータを予め設定された順序で前記複数のデータ処理手段に送出するワークフローシステムであって、前記複数のデータ処理手段はそれぞれ、前記使用者識別子が予め登録されている使用者識別子と一致した場合のみ、前記任意のデータの受信に応じて承認・非承認の判定を受け付ける手段を有することを特徴とする請求項1記載のコンピュータネットワークシステム。

【請求項4】 前記コンピュータネットワークシステムは、任意のデータを予め定められた順序で前記複数のデータ処理手段に送出するワークフローシステムであって、前記通信手段に接続され、前記通信手段を介して受け取った使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する照合手段を具備し、前記複数のデータ処理手段はそれぞれ、アクセス要求に応じて前記使用者識別子を送出し、前記照合手段がアクセス要求可と判定した場合のみ、前記データの受信に応じた承認・非承認の判定を受け付ける手段を有することを特徴とする請求項1記載のコンピュータネットワークシステム。

【請求項5】 前記複数のデータ処理手段はそれぞれ、アクセス要求に応じ、前記使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する手段を有することを特徴とする請求項1記載のコンピュータネットワークシステム。

【請求項6】 前記複数のデータ処理手段はそれぞれ、他のデータ処理手段からのアクセス要求に応じ、このアクセス要求元のデータ処理手段から使用者識別子を受取り、前記予め登録された使用者識別子と照合してアクセ

ス要求の可否を判定する手段を有することを特徴とする請求項5記載のコンピュータネットワークシステム。

【請求項7】 前記生成された特徴データは、一次元射影であることを特徴とする請求項1記載のコンピュータネットワークシステム。

【請求項8】 前記測定手段は、線状電極アレイを有し、前記生成手段は、前記線状電極アレイに前記使用者の指が載置された際、隣接した各線状電極の抵抗値の分布を検出することを特徴とする請求項1記載のコンピュータネットワークシステム。

【請求項9】 前記照合手段は、前記使用者識別子と、前記予め登録された使用者識別子との位置合わせを行い、位置合せされた前記使用者識別子と前記予め登録された使用者識別子との相違度を算出し、算出された相違度と予め設定されたしきい値とを比較してアクセス可否を判定することを特徴とする請求項2記載のコンピュータネットワークシステム。

【請求項10】 複数のデータ処理手段と、この複数のデータ処理手段を相互接続する通信手段とを有するネットワークシステムにおけるアクセス管理方法であって、アクセス要求に応じ、使用者の身体的特徴を測定するステップと、測定された身体的特徴を縮退して特徴データを生成するステップと、前記特徴データを使用者識別子として前記通信手段を介して送受するステップとを具備することを特徴とするアクセス管理方法。

【請求項11】 前記通信手段を介して送受される前記使用者識別子を、予め登録された使用者識別子と照合するステップと、前記照合ステップの照合結果に従って、アクセス要求の可否を判定するステップとを具備することを特徴とする請求項10記載のアクセス管理方法。

【請求項12】 前記生成ステップにより生成された特徴データは、一次元射影であることを特徴とする請求項10記載のアクセス管理方法。

【請求項13】 前記照合ステップは、前記使用者識別子と、前記予め登録された使用者識別子との位置合わせを行うステップと、位置合せされた前記使用者識別子と前記予め登録された使用者識別子との相違度を算出するステップと、算出された相違度と予め設定されたしきい値とを比較するステップとを有することを特徴とする請求項11記載のアクセス管理方法。

【請求項14】 複数のデータ処理装置が相互接続されたネットワークシステムにおける個人認証装置であって、基板上に一次元に配列された線状電極アレイのアレイ方向に沿って被認証者の指が接触することによる前記線状

10

20

30

40

50

## 3

電極アレイの隣接電極間の抵抗値の分布に基づいて特徴データを出力する特徴抽出手段と、

前記特徴抽出手段から出力される特徴データと予め登録されている特徴データとの位置合わせ処理を行う位置合わせ手段と、

この位置合せ手段により位置合わせれた前記特徴データと前記登録された特徴データとの相違度を算出する相違度計算手段と、

相違度計算手段により算出された相違度と予め設定されたしきい値とを比較して前記被認証者の認証を判定する判定手段とを具備することを特徴とする個人認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、複数のコンピュータシステムが通信網を介して相互に接続されることにより構成されるコンピュータネットワークシステム、このコンピュータネットワークシステムにおけるアクセス管理方法、及びこのコンピュータネットワークシステムにおいて使用される個人認証装置に関し、特に、使用者の身体的特徴データを用いてセキュリティ処理を行うコンピュータネットワークシステム、このコンピュータネットワークシステムにおけるアクセス管理方法、及びこのコンピュータネットワークシステムにおいて使用される個人認証装置に関する。

【0002】

【従来の技術】複数のコンピュータ端末（システム）を通信網により相互に接続したコンピュータネットワークシステムでは機密保護のため、ネットワークシステムへのアクセス要求に応じて、使用者を識別してアクセス権の有無を判定する処理、即ちアクセスの許可判定処理を行う必要がある。

【0003】使用者を識別する方法としては、使用者識別子としてパスワードをコンピュータ端末のキーボードから入力する方法が最も一般的に用いられている。しかし、この方法ではキーボードから入力されるパスワードのみが使用者識別の判定基準であるため、使用登録者以外でもパスワードを知りさえすればネットワークにアクセスでき、不正なアクセスを完全に防止することはできない。

【0004】従って、セキュリティを向上させるためにパスワードを複雑にしたり、ネットワーク内の各コンピュータシステムから他のコンピュータシステムにアクセスする際には個別に専用パスワードを設定する等の対策が施されている。しかし、この方法では使用者が複雑なパスワードを複数種類記憶する必要があり、更にパスワードの入力操作も非常に手間がかかるため、使用者の負担が大きい。

【0005】

【発明が解決しようとする課題】上述したように、コンピュータネットワークシステムにおいて、パスワードを

## 4

用いてネットワークシステムまたはコンピュータシステムにアクセスを行う従来の方式では、完全な機密保護が困難であり、かつ使用者の操作が煩雑であるという問題点がある。

【0006】この発明は上述した実情に鑑みてなされたものであり、身体的特徴データを用いることにより、使用者からのアクセス要求に応じてアクセス権の有無を判別する処理を高速に行うことができ、且つ、確実に機密保護を維持することが可能なコンピュータネットワークシステムを提供することを目的とする。

【0007】又、この発明は、コンピュータネットワークシステムにおいて、身体的特徴データを用いることにより、使用者からのアクセス要求に応じてアクセス権の有無を判別する処理を高速に行うことができ、且つ、確実に機密保護を維持することが可能なアクセス管理方法を提供することを目的とする。

【0008】又、この発明は、容易な操作で確実な認証処理を行い、使用者の負担を軽減することができる、コンピュータネットワークシステムにおいて使用される個人認証装置を提供することを目的とする。

【0009】

【課題を解決するための手段】この発明に係るコンピュータネットワークシステムは、複数のデータ処理手段と前記複数のデータ処理手段を相互接続する通信手段とにより構成されるコンピュータネットワークシステムであって、前記複数のデータ処理手段はそれぞれ、使用者の身体的特徴を測定する測定手段と、測定された身体的特徴を縮退して特徴データを生成する生成手段と、前記特徴データを使用者識別子として前記通信手段を介して送受するデータ送受手段とを具備することを特徴とする。

【0010】前記コンピュータネットワークシステムにおいて、前記複数のデータ処理手段は、アクセス要求に応じて前記使用者識別子を送出し、前記通信手段に接続され、前記通信手段を介して受け取った使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する照合手段を具備することを特徴とする。

【0011】この発明に係るアクセス管理方法は、複数のデータ処理手段と、この複数のデータ処理手段を相互接続する通信手段とを有するネットワークシステムにおけるアクセス管理方法であって、アクセス要求に応じ、使用者の身体的特徴を測定するステップと、測定された身体的特徴を縮退して特徴データを生成するステップと、前記特徴データを使用者識別子として前記通信手段を介して送受するステップとを具備することを特徴とする。

【0012】前記アクセス管理方法は更に、前記通信手段を介して送受される前記使用者識別子を、予め登録された使用者識別子と照合するステップと、前記照合ステップの照合結果に従って、アクセス要求の可否を判定す

## 5

るステップとを具備することを特徴とする。

【0013】以上のコンピュータネットワークシステム、またはアクセス管理方法においては、人間の身体的特徴、例えば指の特徴を抽出して得られる特徴データは指紋に依存するものであり、各個人に固有のものである。従って、この特徴データを使用者識別子として用いてネットワークシステムに対するアクセス権の有無を判定すれば、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護ができ、かつ煩雑な入力操作を必要としないので、アクセス操作における使用者の負担が軽減される。

【0014】又、このシステムで用いられる特徴データは縮退されたデータであり、一般的な指紋画像を用いるものに比べて、データ量が約10分の1となり、ネットワーク上での通信網を介した転送や、照合サーバでの照合等の処理を高速で行うことができる。同様に、照合処理に必要なとされるファイルシステムの容量も従来の約10分の1でよい。

【0015】又、このようなコンピュータネットワークシステムにおいて、一度ネットワークへのアクセスが認められた場合、指の特徴データがあるコンピュータシステムから他のコンピュータシステムにアクセスする際の使用者識別子として使用することにより、従来のように他のコンピュータシステムにアクセスする際に必要としていた煩わしい手順が簡略化される。

【0016】又、前記複数のデータ処理手段はそれぞれ、アクセス要求に応じ、前記使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する手段を有する構成であってもよい。更に、前記複数のデータ処理手段はそれぞれ、他のデータ処理手段からのアクセス要求に応じ、このアクセス要求元のデータ処理手段から使用者識別子を受取り、前記予め登録された使用者識別子と照合してアクセス要求の可否を判定する手段を有する構成であってもよい。

【0017】前記生成された特徴データは、一次元射影等の縮退されたデータである。又、前記測定手段は、線状電極アレイを有し、前記生成手段は、前記線状電極アレイに前記使用者の指が載置された際、隣接した各線状電極の抵抗値の分布を検出する構成であってもよい。

【0018】前記照合手段または照合ステップは、前記使用者識別子と、前記予め登録された使用者識別子との位置合わせを行い、位置合せされた前記使用者識別子と前記予め登録された使用者識別子との相違度を算出し、算出された相違度と予め設定されたしきい値とを比較してアクセス可否を判定することが好ましい。

【0019】又、前記発明に係るコンピュータネットワークシステムは、任意のデータを予め設定された順序で前記複数のデータ処理手段に送出するワークフローシステムであって、前記複数のデータ処理手段はそれぞれ、前記使用者識別子が予め登録されている使用者識別子と

## 6

一致した場合のみ、前記任意のデータの受信に応じて承認・非承認の判定を受け付ける手段を有することを特徴とする。

【0020】従って、コンピュータネットワークシステム上に設定された一連の仕事の流れを運用するワークフローシステムにおいて、予め設定した条件によって承認・非承認の判定を行う判定処理の際に、予め登録してある指の特徴データと判定時に入力された指の特徴データが一致した場合のみに判定処理を行うことができるようにすることで、操作が容易でかつ確実な電子承認が可能となる。

【0021】前述した測定部及び生成部は、線状電極アレイのアレイ方向に沿って使用者の指が接触することによる隣接電極間の抵抗値の分布から指の特徴を抽出して、指の長手方向に沿った一次元の特徴抽出データを出力する。従って、指紋を2次元の画像として検出する指紋センサに比較して特徴データのデータ量が著しく少ないため、コンピュータネットワークシステム上での転送や登録されている特徴データとの照合処理を高速に行うことができ、従って迅速に個人認証を行うことが可能となる。

【0022】この発明に係る個人認証装置は、複数のデータ処理装置が相互接続されたネットワークシステムにおける個人認証装置であって、基板上に一次元に配列された線状電極アレイのアレイ方向に沿って被認証者の指が接触することによる前記線状電極アレイの隣接電極間の抵抗値の分布に基づいて特徴データを出力する特徴抽出手段と、前記特徴抽出手段から出力される特徴データと予め登録されている特徴データとの位置合わせ処理を行う位置合わせ手段と、この位置合せ手段により位置合わせされた前記特徴データと前記登録された特徴データとの相違度を算出する相違度計算手段と、相違度計算手段により算出された相違度と予め設定されたしきい値とを比較して前記被認証者の認証を判定する判定手段とを具備することを特徴とする。

【0023】これにより、指紋を2次元の画像として検出する指紋センサに比較して特徴データのデータ量が著しく少ないため、コンピュータネットワークシステム上での転送や登録されている特徴データとの照合処理を高速に行って、迅速な個人認証が可能であると共に、被認証者の指と線状電極アレイの相対位置が登録時と多少異なっても、位置合わせ処理を行うことにより、抽出された特徴データと登録されている特徴データとの比較照合を正確に行うことができる。

【0024】

【発明の実施の形態】以下、この発明に係る第1の実施の形態～第4の実施の形態を図面を参照して説明する。図1は、この発明の第1の実施の形態に係るコンピュータネットワークシステム10の概略構成を示すブロック図である。同図に示されるように、複数のコンピュータ

システム11(11-1~11-3)が通信網12を介して相互に接続されている。各コンピュータシステム11にはそれぞれデータ縮退ユニット13(13-1~13-3)を介し、使用者の身体的特徴(特徴データ)を計測する特徴計測ユニット14(14-1~14-3)がそれぞれ接続されている。このデータ縮退ユニット13及び特徴計測ユニット14により使用者の身体的特徴が電気信号として抽出される。

【0025】尚、この実施の形態では、特徴計測ユニット14は、使用者の身体的特徴として後述するように使用者の指の指紋情報を測定する。身体的特徴とは、人間の身体に係る情報であって、各個人に固有の特徴を意味する。又、図1に示されるコンピュータネットワークシステム10には、3つのコンピュータシステム11が接続されているが、接続されるコンピュータシステムの数にはこれに限定されない。

【0026】通信網12には、更に、各特徴計測ユニット14により測定された特徴データに基づいてコンピュータネットワークシステムに対する使用者のアクセス権の有無を識別する照合サーバ15が接続されている。この照合サーバ15はコンピュータシステム11から通信網12を介して送られる縮退された特徴データ(以降、抽出特徴データと称する)と、このコンピュータネットワークシステムにおいて予め登録されている指の特徴データ(以降、登録特徴データと称する)とを照合し、使用者つまり被認証者がアクセス権を有するか否かを判定する。

【0027】尚、登録特徴データは、この実施の形態ではファイルシステム16に保持される。次に、前記図1に示されるデータ縮退ユニット13及び特徴計測ユニット14による身体的特徴の抽出処理を図2~図4を参照して説明する。特徴計測ユニット14は、前述したように、識別対象である使用者の指の指紋情報を測定する。データ縮退ユニット13は、特徴計測ユニット14により計測された指紋情報を、抽出特徴データとして電気信号で算出する。この際、フィルタリング処理やアナログ/デジタル変換処理等を施す。このデータ縮退ユニット13により求められた抽出特徴データは、例えば、指の表面画像を示すデータに比べて情報量が少ない、一次元射影等の縮退されたデータである。

【0028】ここで、縮退データについて説明する。通常、指紋画像、顔画像、声、目の網膜等の身体的特徴を測定した時の測定データには、複数の特徴が含まれている。例えば、二次画像は複数の一次画像で構成されている。この複数の特徴の内、幾つかの特徴を演算処理により消去、または他の特徴と等価な値に変換することにより、データ全体の情報量を減ずることを縮退、または縮退処理とし、縮退データとは、このような処理が施されたデータを示す。

【0029】先の演算処理には、専用回路によるデータ

処理や計算、または、専用のデバイス(電極アレイや光学式演算装置等)による測定が該当する。従って、フィルタリング処理もデータの縮退処理とみなすことができる。

【0030】このような縮退処理には、一次元射影(三次元画像の場合は二次元射影)、輪郭の抽出、ベクトル(ベクトルの動き)抽出、フーリエ変換、特徴抽出、スムージング等がある。

【0031】ここで、特徴計測ユニット14及びデータ縮退ユニット13とが一体となった特徴計測及びデータ縮退ユニットの構成例を図2(a)、(b)に示す。図2(a)は、前記一体とされた構成であるユニット上に識別対象である指が載置された場合の側面を示し、図2(b)は、後述する線状電極と、識別対象である指の指紋との載置関係を示す。

【0032】絶縁性の基板141の表面に線状電極アレイ142が形成されている。この線状電極アレイ142は、複数の線状電極を一次元のアレイ状に配列したものである。基板141の材料としては、例えばガラスエポキシその他のプリント基板材料、セラミック板、あるいは絶縁被覆を施した金属薄板などが用いられる。線状電極アレイ142の電極材料としては、例えばCu薄膜、Au薄膜、Niメッキ膜、Pt薄膜あるいはPd薄膜のような、人体の皮膚から出る汗等の体液に侵されにくい導電性材料が用いられる。

【0033】又、この電極材料としては、測定対象が比較的高抵抗であるために絶縁体以外の材料であればどのような材料でも適用可能であり、例えばITO(酸化インジウム・スズ)等の酸化物膜でもよい。電極の形成方法に関しても特に制限はなく、メッキ・蒸着等通常の方法はいずれも適用することができる。

【0034】線状電極アレイ142には使用者の指が接触されるので、電極間隔は数百 $\mu\text{m}$ 程度の指紋ピッチ、即ち指紋を構成する凹凸ピッチ(約0.5mm)より細かいピッチとし、例えば0.1mm程度とする。また、線状電極アレイ142のアレイ方向の長さ(アレイ長)は、指の先端から第二関節を完全に含む長さとする。電極間隔は一定なので、アレイ長は電極数によって調整することができる。

【0035】線状電極アレイ142を構成する各々の電極には、引き出し端子144が接続されている。特徴測定時には、図2(a)、(b)に示されるように、指143を線状電極アレイ142のアレイ方向に沿って、即ち電極の個々の長手方向に直交するように押し付ける。

【0036】一体化されたデータ縮退ユニット13及び特徴計測ユニット14の価回路を図3に示す。特徴計測及びデータ縮退ユニットは、前記引き出し端子144に接続されているスイッチ回路145、基準抵抗 $R_{\text{ref}}$ 、及び低電圧源 $V_0$ を有し、前記図2(a)、(b)に示される線状電極アレイ142(図3では、 $n$ 本の電極1

42-1~142-nとして示している)上に指を押し付けたときの隣接する電極間の抵抗値を指の長さ方向に順次読み取る。

【0037】通常、人間の指の表面は、汗口の配列に従って皮膚が隆起して指紋を形成しており、この汗口からは、常時汗が自然放散している。即ち、指紋凸部からは常にNaやClを微量に含む水分の放散がある。従って、線状電極アレイ142上に指が押し付けられると、指紋凸部の汗口から放散された水分(発汗)は、指紋凸部直下の線状電極に到達する。この時、水分が到達した電極間では、水分に依存するイオンにより電気抵抗が低下する。ゆえに、指紋の凸部に対応した部分のみがそれ以外の部分に比べて低抵抗の状態となる。

【0038】このような発汗に応じた低抵抗状態の他にも、状電極アレイ142に識別対象となる使用者の指が押し付けられると、隣接する2つの電極142i、142i+1(i=1, 2, ..., n)間のスペースに指紋を形成する凸部が入り込む形となる。この場合、隣接する2つの電極142i、142i+1間の抵抗値Riは、その電極間スペースに入り込む指の凸部の量に応じても変化することになる。つまり、電極間スペースに入り込む凸部の量が多ければ、それだけ抵抗値Riは低くなる。

【0039】電極142-1~142-nには、引き出し端子144を介してスイッチ回路145が接続されている。スイッチ回路145は、アナログスイッチ、さらに具体的にはアナログマルチプレクサIC(integrated circuit)を用いて構成してもよい。スイッチ回路145は、隣接する2つの電極142i、142i+1を基準抵抗Rrefを介して定電圧源Voに接続する。

【0040】例えば、図3の状態では破線で示されるように、電極142-1と142-2が基準抵抗Rrefを介して定電圧源Voに接続されている。基準抵抗Rrefの両端の電位差Viは、次式で与えられる。

【0041】 $V_i = R_{ref} \cdot V_o / (R_{ref} + R_i)$   
スイッチ回路145により、この電位差Viを検出すべき隣接する2つの電極の組み合わせを142-1と142-2、142-2と142-3、...142-n-1と142-nと順次切り替えて、電位差Viを指の長さ方向に順次読み取る。このようにして読み取られる電位差Viを時系列にプロットすると図4に示すようになり、指の長手方向への多値射影と等価なパターンが得られる。なお、図4で横軸は隣接する2つの電極の位置を示し、縦軸は電位差Viを示している。

【0042】前述したよ処理により得られた信号は、特徴計測及びデータ縮退ユニットにおいて更に、フィルタリングおよびアナログ-デジタル変換が行われる。ここで、データ縮退ユニット13から出力されるデータは、例えば、電極間の検出分解能を8ビットとした場合には約100バイト程度のデータ量となる。このデータ

を示す信号パターンをA(i)とする。

【0043】又、ここで求められた特徴データは、一般的な指紋画像を用いるものに比べて、大きさ(データ量)が約一桁も小さいため、図1のコンピュータネットワーク上での通信網12を介しての転送や、照合サーバ15での照合等の処理を高速で行うことができるという大きな利点を有している。

【0044】例えば、人間の指の指紋画像では、指紋画像は圧縮処理が施された場合であっても、通常、1Kバイト程度のデータ量となる。本願では、前述したように人間の身体的特徴を縮退することにより、指紋情報であれば、約100バイトで、指紋画像の約10分の1のデータ量でよい。同様に、照合処理に必要とされるファイルシステム16の容量も従来の約10分の1でよい。

【0045】次に、照合サーバ15について説明する。図5は照合サーバ15の構成を示す機能ブロック図である。照合サーバ15は、位置合わせ処理部151、相違度計算部152および比較部153により構成される。

【0046】位置合わせ処理部151は、特徴計測ユニット14及びデータ縮退ユニット13により抽出された抽出特徴データを表わす信号パターンA(i)と、ファイルシステム16から読み出された登録特徴データを表わす登録信号パターンAd(i)との位置合わせを行う。

【0047】ファイルシステム16に保持されている登録特徴データは、特徴計測ユニット14において、指を線状電極アレイ142上にある一定の状態に置いたときに得られた特徴データである。しかし、照合処理を行うために計測をする場合、即ち、抽出特徴データを得るとき、特徴計測ユニット14上で使用者が指を置く状態は、登録特徴データを得たときと同じとは限らない。即ち、指を載置する位置が微妙に異なることが予想される。

【0048】そこで、位置合わせ処理部151では、抽出特徴データを登録特徴データを得たときと同じ位置状態で得たデータとなるように、位置合わせ処理を行う。この処理によって、照合をより確実に行うことができる。位置合わせ処理の具体的な手法は後述する。

【0049】相違度計算部152は、位置合わせ処理部151の出力信号から抽出特徴データと登録特徴データとの相違度を計算する。当然のことながら、この相違度が小さいほど特徴測定ユニット14及びデータ縮退ユニット13において、特徴が抽出された被認証者は、予めファイルシステム16の登録されている使用者本人である可能性が高いことになる。

【0050】比較部153は、相違度計算部152で求められた相違度をあるしきい値THと比較することによって、被認証者が登録されている本人かどうか、つまりアクセス権を有する使用者か否かを判定する。



【0051】上述したこの第1の実施の形態の構成において、コンピュータシステム11を介してコンピュータネットワークシステム10にアクセスしようとする使用者は、まず、そのコンピュータシステム11に接続された特徴計測ユニットを介して指の特徴を入力する。特徴計測ユニット14及びデータ縮退ユニット13により得られた抽出特徴データは、通信網12を介して前記図5に示されるような構成を有する照合サーバ15に転送され、この照合サーバ15において予めファイルシステム16に登録されている登録特徴データと比較照合される。この比較照合によって、使用者のアクセス権の有無が判定される。

【0052】照合サーバ15での照合処理は、図6に示すフローチャートに従って行われる。先ず、位置合わせ処理部151で位置合わせ処理が行われる。即ち、アクセスを要求するコンピュータシステム11から送られた

$m \geq 0$  のとき

$$S(m) = \frac{1}{N-m} \sum_{i=1}^{N-m} \{A(i+m) - Ad(i)\}^2 \quad (1)$$

$m < 0$  のとき

$$S(m) = \frac{1}{N+m} \sum_{i=-m+1}^N \{A(i+m) - Ad(i)\}^2 \quad (2)$$

【0055】この加算値  $S(m)$  は、 $A(i+m)$  と  $Ad(i)$  との一致度を表わすパラメータであり、この  $S(m)$  の値が小さいほど一致していることを示す。 $m$  を所定の範囲で変化させ、 $S(m)$  の値が最小となるときの  $m$  を位置ずれ量  $M$  とし、この位置ずれ量  $M$  だけシフトしたパターン  $A(i)$  を、即ち、パターン  $A(i+M)$

$M \geq 0$  のとき

$$E = \frac{\sum_{i=1}^{N-M} \{A(i+M) - Ad(i)\}^2}{\sum_{i=1}^{N-M} Ad(i)^2} \quad (3)$$

$M < 0$  のとき

$$E = \frac{\sum_{i=-M+1}^N \{A(i+M) - Ad(i)\}^2}{\sum_{i=-M+1}^N Ad(i)^2} \quad (4)$$

【0057】このような式で求められる相違度  $E$  は、位置合わせされた入力信号パターン  $A(i+M)$  と登録信号パターン  $Ad(i)$  の2乗誤差を所定の範囲にわたって加算したものを同じ範囲の登録信号パターン  $Ad(i)$  の2乗和で正規化したものを示す。この相違度  $E$  は位置合わせされた入力信号パターン  $A(i+M)$  と登録

抽出特徴データである信号パターン  $A(i)$  が入力される(ステップS11)。更に、この信号パターン  $A(i)$  と、照合サーバ15がファイルシステム16から読み出した登録特徴データである登録信号パターン  $Ad(i)$  とを用い、 $A(i)$  を  $m$  だけずらした信号パターン  $A(i+m)$  と登録信号パターン  $Ad(i)$  との2乗誤差を所定の範囲にわたって加算される(ステップS12)。

【0053】この加算値を  $S(m)$  とすると、これは  $m$  の値の範囲によって次式(1)(2)のいずれかとなる。なお、 $m \geq 0$  は指を例えば指先方向にシフトした状態に相当するものとする、 $m < 0$  は指をこれと逆方向つまり根元方向にシフトした状態に相当する。

【0054】

【数1】

において位置合わせができると判定する(ステップS13)。次に、相違度計算部152において、相違度  $E$  が次式(3)(4)により求められる(ステップS14)。

【0056】

【数2】

信号パターン  $Ad(i)$  との相違度を表したもので、 $E$  の値が大きいほど両信号の違いが大きく、値が小さいほど両信号が似ていることを示す。

【0058】次に、比較部153において、相違度  $E$  が予め定められたしきい値  $TH$  と比較され(ステップS15: S16)、 $E \leq TH$  ならば両信号は一致しており、

アクセスを使用として使用者である被認証者を本人と判断して照合処理を終了する（ステップS17）。また、 $E > TH$ ならば両信号が一致していないと判断し、被認証者を他人と判断して照合処理を終了する（ステップS18）。

【0059】前記ステップS17で被認証者を本人と判断すると、照合サーバ15はその被認証者つまり使用者にアクセス許可を与える。照合サーバ15は、全てのネットワーク上のアクセス条件が設定されており、ネットワーク内のあるコンピュータシステムが同じネットワーク内の他のコンピュータシステム（サービス）にアクセスを要求する際にも、上述のようにして抽出された特徴データを使用者識別子を用い、照合・判定処理を行うことができる。

【0060】以上説明したように、この第1の実施の形態によれば人間の身体的特徴を示す（この第1の実施の形態では指の指紋）特徴を抽出して得られる特徴データを使用者識別子として、予め登録されている特徴データと比較照合することでネットワークシステムに対するアクセス権の有無が判定される。

【0061】これにより、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護を実現できる。また、特徴データの抽出には使用者が例えば実施の形態で説明したような線状電極アレイ上に指を押し付けるといった簡単な操作を行えばよく、パスワード入力のような煩雑な入力操作を必要としないので、アクセス操作における使用者の負担を大きく軽減することができる。

【0062】又、この第1の実施の形態で用いられる特徴データは縮退されたデータであり、一般的な指紋画像を用いるものに比べて、データ量が約10分の1となり、図1のコンピュータネットワーク上での通信網12を介しての転送や、照合サーバ15での照合等の処理を高速で行うことができる。同様に、照合処理に必要とされるファイルシステム16の容量も従来の約10分の1でよい。

【0063】前記特徴データの抽出には、従来適用されている光学方法では、図7（a）に示されるような各種処理が必要とされる。まず、光学センサによって2次元情報である指画像が取り込まれ、取り込まれた指画像の指の横方向の画素情報が加算される（ステップS21、S22）。この後、バンドパスフィルタを用いて加算された情報の高周波成分及び低周波成分が除去され、特徴データとして出力される（ステップS23、S24）。

【0064】一方、前述した電極アレイを用いた方法では、図7（b）に示されるように、指の抵抗値分布の検出（ステップS31）と、高周波成分・低周波成分の除去（ステップS32）とを行った後に特徴データが出力され（ステップS33）、従来の光学方法に比べて少ない処理で特徴データを出力することができる。このた

め、各コンピュータシステム11に接続されたデータ縮退ユニット13及び特徴計測ユニット14において迅速な特徴データの抽出が可能となる。

【0065】この第1の実施の形態においては、人間の身体的特徴を示す縮退された特徴データとして指の指紋の一次元射影を用いたが、この他、指の輪郭や、フーリエ変換を用いて求めた指紋情報を適用することもできる。

【0066】また、一度このようにしてネットワークへのアクセスが認められた場合、指の特徴データのあるコンピュータシステムから他のコンピュータシステムにアクセスする際の使用者識別子として使用することにより、他のコンピュータシステムにアクセスする際に従来必要としていた複数種類のパスワード入力のような煩わしい手順を簡略化することができる。

【0067】前述した電極アレイ式では、特徴計測ユニットと縮退ユニットとが一体のユニットとなる構成であった。しかし、例えば、1次元射影を検出する光学式の装置を適用しても良い。この場合には、図8（a）に示されるように、特徴計測ユニットとデータ縮退ユニットとを異なるユニットで構成することができる。同図に示されるように、特徴計測ユニットは、光学式指紋測定器により構成され、データ縮退ユニットは、一次元射影計算部及びフィルタリング・A/D変換部により構成される。

【0068】光学式指紋画像測定器は、図8（b）に示されるような2次元の指紋画像の測定を行い、測定された画像情報を一次元射影計算部に送る。一次元射影計算部では、2次元の画像情報を一次元の情報に計算すると共に、フィルタリング処理や、A/D変換を行うことにより、抽出された特徴を含む縮退データを出力する。

【0069】前述した第1の実施の形態では、データ縮退ユニット13を介してコンピュータシステム11と特徴計測ユニット14とが接続された構成となっているが、データ縮退ユニット13及び特徴計測ユニット14をコンピュータシステム11に組み込んだ構成としてもよい。例えば、特徴計測ユニット14と同様の機能を有する特徴計測部をコンピュータシステム11のキーボード上に配設してもよい。

【0070】このように、データ縮退ユニット13と特徴計測ユニット14とを、特徴抽出部としてコンピュータシステム11に組み込んだ場合、前述したコンピュータネットワークシステムは図9に示されるような構成となる。

【0071】ここでは、前述した第1の実施の形態と同様に、複数のコンピュータシステム21（21-1～21-3）が通信網22を介して相互に接続されている。各コンピュータシステム21には、使用者の身体的特徴（特徴データ）を抽出する特徴抽出部27（27-1～27-3）がそれぞれ内蔵されている。この特徴抽出部

27の機能は、前述した特徴計測ユニット14及びデータ縮退ユニット13の有する機能と同様であり、抽出された特徴データは、縮退されたデータである。

【0072】通信網22には、更に、各特徴計測ユニット24により測定された特徴データに基づいてコンピュータネットワークシステムに対する使用者のアクセス権の有無を識別する照合サーバ25が接続されている。

【0073】図9に示されるコンピュータネットワークシステム20における動作は、前述した第1の実施の形態の動作と同様であるので詳細な説明は省略する。又、コンピュータネットワークシステム20においても、第1の実施の形態と同様の効果を得ることができる。

【0074】次に、この発明に係るコンピュータネットワークシステムの第2の実施の形態を説明する。この第2の実施の形態では、この発明をワークフローシステム(workflow system)に適用する。

【0075】図10は、この第2の実施の形態におけるワークフローの処理を示すフローチャートである。この第2の実施の形態に係るコンピュータネットワークシステムは、前記図1に示される第1の実施の形態の構成と同様の構成を有する。

【0076】このコンピュータネットワークシステムは、ワークシステム上に設定された一連の仕事の流れを運用するワークフローシステムであり、電子承認が必要な処理を行うコンピュータシステム11に、身体的特徴を抽出するための、データ縮退ユニット13及び特徴抽出ユニット14が接続されており、照合サーバ15のファイルシステム16には承認権利を有する人の特徴データ(例えば、指の指紋情報)および処理条件が登録されている。

【0077】以下、図10を用いて具体的に処理の流れを説明する。尚、ここでは、前述した第1の実施の形態と同様に特徴データとして、人間の指の指紋情報を適用する。

【0078】設定された一連の仕事の流れの中で、承認手続き要求が発生した場合、要求された使用者のコンピュータシステム11は通信網12を介して承認手続き要求を受信する(ステップS41)。承認者は、受信した要求手続きを端末に表示させ、特徴計測ユニット14を介して指の特徴を入力する(ステップS42)。抽出された特徴データは通信網12を介して照合サーバ15へ送信される。

【0079】照合サーバ15では、図6を用いて説明した照合処理が行われる。これにより、ファイルシステム15に予め承認権利有資格者として登録してある特徴データと、送信された抽出特徴データが一致した場合、承認・非承認手続きを実行することが可能であるとして前記コンピュータシステム11に許可が与えられる(ステップS43)。承認手続き処理が実行された後、通信網12を介して次の処理に該当するコンピュータシステム

11に処理データが送られる(ステップS44、S45)。

【0080】尚、ここでは承認手続きに関して説明したが、計算や文書追加等他の処理に関しても、処理実行者を限定したい場合は同様にこの発明を適用することが可能である。

【0081】さらに、コンピュータネットワークシステム上に設定された一連の仕事の流れを運用するワークフローシステムにこの発明を適用すれば、予め設定した条件によって承認・非承認の判定を行う判定処理の際に、予め登録してある指の特徴データと判定時に入力された指の特徴データが一致した場合のみに判定処理を行うことができるため、簡単な操作で確実な電子承認が可能となる。

【0082】そして、この発明における指の特徴抽出手段では、線状電極アレイのアレイ方向に沿って使用者の指が接触することによる隣接電極間の抵抗値の分布から指の特徴を抽出して、指の長手方向に沿った一次元の特徴抽出データを出力するものであることから、指紋を2次元の画像として検出する指紋センサに比較して特徴データのデータ量が著しく少ないため、コンピュータネットワークシステム上での転送や登録されている特徴データとの照合処理を高速に行うことができ、従って迅速に個人認証を行うことが可能となる。

【0083】次に、この発明に係るコンピュータネットワークシステムの第3の実施の形態を図11～図13を参照して説明する。図10に示されるコンピュータネットワークシステム30は、複数のコンピュータシステム31(31-1～31-3)が通信網32を介して相互に接続されている。各コンピュータシステム31にはそれぞれデータ縮退ユニット33(33-1～33-3)を介し、使用者の身体的特徴(特徴データ)を計測する特徴計測ユニット34(34-1～34-3)がそれぞれ接続されている。このデータ縮退ユニット33及び特徴計測ユニット34により使用者の身体的特徴が電気信号として抽出される。

【0084】尚、この実施の形態では、抽出される身体的特徴を特に限定しないが、例えば、前述した第1の実施の形態と同様に、使用者の指の指紋情報(一次元射影)を測定してもよく、この他、フーリエ変換、輪郭抽出による縮退された特徴データを適用することができる。更に、前記第1の実施の形態と同様に、接続されるコンピュータシステムの数はこれに限定されない。

【0085】前記図1に示されるコンピュータネットワークシステム10と異なる第1の点は、身体的特徴を照合するための照合サーバ15、及びこの照合サーバにより参照される登録特徴データを格納するファイルシステム16がもうけられていないことである。第2の相違点は、通信網32に接続されている各コンピュータシステム31に、それぞれファイルシステム35(35-1～

35-3)が接続されていることである。

【0086】このファイルシステム35は、アクセス権の有無を判定するための照合処理の際に参照される登録特徴データ、及び処理対象となる各種ファイル・データを格納する。従って、この第3の実施の形態では、特徴データの抽出に応じ、先ず、各コンピュータシステム31においてアクセス権の有無を判定するための照合処理を行うことができる。

【0087】次に、図12及び図13に示されるフローチャートを参照して、この第3の実施の形態のコンピュータネットワークシステム30のファイルアクセス動作について説明する。

【0088】コンピュータネットワークシステム30において、任意のコンピュータシステム31でファイルのアクセス要求が発生すると、このコンピュータ31では、特徴計測ユニット34を用いて身体的特徴、例えば指の指紋等を入力するように要求される。ここで、使用者の指等が特徴ユニット34に載置されると、前述した第1の実施の形態における処理と同様に特徴計測ユニット34及びデータ縮退ユニット33により縮退された特徴データが抽出される(ステップS51、S52)。

【0089】抽出された特徴データ(抽出特徴データ)は、アクセス要求の発生した日時や、パスワード等の使用者識別子に付加される(ステップS53)。尚、日時やパスワード等の識別子を付与せず、縮退された抽出特徴データのみを用いても良い。

【0090】次に、コンピュータシステム31では、アクセス要求されたファイルがこのコンピュータシステム31に接続されているファイルシステム35に格納されているか否か判定する(ステップS54)。ここで、ファイルシステム35にアクセス要求されたファイルが格納されている場合、ファイルシステム35に格納されている登録特徴データと、前記抽出特徴データ及び使用者識別子とが同一であるか照合処理が行われる(ステップS56)。

【0091】ここで行われる照合処理は、前述した第1の実施の形態における照合処理等を適用することができる。照合処理の結果が一致である場合、使用者に対し、ファイルアクセスが許可される(ステップS57)。一致でない場合、ファイルアクセスが不可能である通知等がなされた後、ファイルアクセス要求に応じた処理が終了する。

【0092】前記ステップS54において、ファイルシステム35にアクセス要求されたファイルが格納されていない場合、コンピュータシステム31は、アクセス要求するファイルのファイル名等と共に前記抽出特徴データ及び使用者識別子を、通信網32を介して他のコンピュータシステムに送出する(ステップS58)。この後、抽出特徴データ等を送出した送り先のコンピュータシステムからの応答を受信し、アクセスの可否に応じて

前述したような処理を行う(ステップS59)。

【0093】尚、後述するがアクセス可の場合、アクセス要求したファイルが送られるので、これをファイルシステム35に格納する等の処理も行われる。次に、前記ステップS58において送出された各種データを受信したコンピュータシステム31の処理を図13を参照して説明する。

【0094】コンピュータシステム31は、他のコンピュータシステムから、アクセス要求するファイルのファイル名等と共に前記抽出特徴データ及び使用者識別子を受信すると、アクセス要求されているファイルが自コンピュータシステム31に接続されているファイルシステム35に格納されているか否か判定する(ステップS61、S62)。ここで、ファイルシステム35に要求されたファイルが格納されていない場合、この旨を要求元のコンピュータシステムに通知する(ステップS63)。

【0095】前記ステップS62において、アクセス要求されたファイルがファイルシステム35に格納されている場合、ステップS61において受信した抽出特徴データ及び使用者識別子を用い、要求元の使用者にファイルアクセス権が有るか否かを決定するための照合処理を行う(ステップS64、S65)。照合結果が一致である場合、要求元のコンピュータシステムに対し、アクセス権を有することを通知すると共に、アクセス要求されたファイルを送出する(ステップS66)。照合結果が不一致である場合、ファイルのアクセス権が無いことを要求元のコンピュータシステムに通知する(ステップS67)。

【0096】以上説明したように、この第3の実施の形態によれば人間の身体的特徴を示す特徴を抽出して得られる特徴データを使用者識別子として、予め登録されている特徴データと比較照合することでネットワークシステムに対するアクセス権の有無が判定される。これにより、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護を実現できる。

【0097】特に、この第3の実施の形態では、通信網32に接続されている各コンピュータシステムにおいて、先ず、ファイルアクセス要求に応じたアクセス権の有無判定処理が単独で行われ、アクセス要求されたファイルがファイルシステムに格納されていない時のみ、通信網32を介して他のコンピュータシステムにおいてアクセス権の有無判定処理が行われる。このため、アクセス権の有無判定処理を行う度に通信網32を介してデータの送受を行う必要はなく、通信網32上のデータの通信効率を向上することが可能となる。

【0098】又、この第3の実施の形態で用いられる特徴データは、前記第1の実施の形態と同様に縮退されたデータであり、一般的な指紋画像を用いるものに比べ

て、データ量を節約することができる。従って、データの転送や処理を高速に行うことができる。

【0099】次に、この発明に係るコンピュータネットワークシステムの第4の実施の形態を図14及び図15を参照して説明する。図14に示されるコンピュータネットワークシステム40は、基本的に前記図1に示されるコンピュータネットワークシステム10と同様であるので詳細な説明は省略する。但し、このコンピュータネットワークシステム40は、前述した第3の実施の形態と同様に、通信網42に接続されている各コンピュータシステム41に、それぞれファイルシステム47（47-1～47-3）が接続されている。

【0100】但し、このファイルシステム47は、処理対象となる各種ファイル・データのみを格納する。従って、この第4の実施の形態では、前記第1の実施の形態と同様に、特徴データの抽出に応じ照合サーバ45に抽出特徴データが送られる。そして、この照合サーバ45において、アクセス権の有無を判定するための照合処理が行われる。

【0101】このコンピュータネットワークシステム40における、ファイルアクセスに応じた、コンピュータシステム41及び照合サーバ45の処理を図15のフローチャートに示す。

【0102】コンピュータネットワークシステム40において、任意のコンピュータシステム41でファイルのアクセス要求が発生すると、このコンピュータ41では、特徴計測ユニット44を用いて身体的特徴、例えば指の指紋等を入力するように要求される。ここで、使用者の指等が特徴ユニット44に載置されると、前述した第1の実施の形態における処理と同様に特徴計測ユニット44及びデータ縮退ユニット43により縮退された特徴データが抽出される（ステップS71、S72）。

【0103】抽出された特徴データ（抽出特徴データ）は、アクセス要求の発生した日時や、パスワード等の使用者識別子に付加され、通信網42を介して照合サーバ45に送出される（ステップS73、S74）。尚、日時やパスワード等の識別子を付与せず、縮退された抽出特徴データのみを用いても良い。

【0104】次に、照合サーバ45では、抽出特徴データ及び使用者識別子の受信に応じ、ファイルシステム45に格納されている登録特徴データと、前記抽出特徴データ及び使用者識別子とが同一であるか照合処理が行われる（ステップS75、S76）。ここで行われる照合処理は、前述した第1の実施の形態における照合処理等を適用することができる。照合処理の結果が一致である場合、使用者に対し、ファイルアクセスが許可され、この旨が通知される（ステップS77、S78）。一致でない場合、ファイルアクセス権無しと判断されこの旨が通知される（ステップS79、S78）。

【0105】以上説明した、この第4の実施の形態によ

れば前記第1の実施の形態と同様の効果を得ることができる。即ち、人間の身体的特徴を示す特徴を抽出して得られる特徴データを使用者識別子として、アクセス権の有無が判定されるので、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護を実現できる。又、用いられる特徴データは、前記第1の実施の形態と同様に縮退されたデータであり、一般的な指紋画像を用いるものに比べて、データ量を節約することができる。従って、データの転送や処理を高速に行うことができる。

【0106】

【発明の効果】以上詳述したように、この発明によれば、コンピュータシステムにおいて、身体的特徴データを用いることにより、使用者からのアクセス要求に応じてアクセス権の有無を判別する処理を高速に行うことができ、且つ、確実に機密保護を維持することが可能となる。

【0107】又、この発明によれば、コンピュータネットワークシステムにおいて使用される個人認証装置において、容易な操作で確実な認証処理を行い、使用者の負担を軽減することができる。

【0108】特に、人間の身体的特徴を示す特徴を抽出して得られる特徴データを使用者識別子として、予め登録されている特徴データと比較照合することでネットワークシステムに対するアクセス権の有無が判定される。これにより、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護を実現できる。また、特徴データの抽出には使用者が例えば実施の形態で説明したような線状電極アレイ上に指を押し付けるという簡単な操作を行えばよく、パスワード入力のような煩雑な入力操作を必要としないので、アクセス操作における使用者の負担を大きく軽減することができる。

【0109】又、この特徴データは縮退されたデータであり、一般的な指紋画像を用いるものに比べて、データ量が約10分の1となり、コンピュータネットワーク上での通信網を介しての転送や、照合サーバ等での照合等の処理を高速で行うことができる。同様に、照合処理に必要とされるファイルシステムの容量も従来の約10分の1でよい。

【図面の簡単な説明】

【図1】この発明の第1の実施の形態に係るコンピュータネットワークシステムの概略構成を示すブロック図。

【図2】前記第1の実施の形態における特徴計測及びデータ縮退ユニットの概略構成を示す図。

【図3】前記第1の実施の形態における特徴計測及びデータ縮退ユニットの等価回路の一例を示す図。

【図4】前記第1の実施の形態における特徴計測及びデータ縮退ユニットにより検出される、縮退済みの指の特徴パターンである、隣接電極間の抵抗値の分布例を示す

10

20

30

40

50

図。

【図5】前記第1の実施の形態における照合サーバの構成を示すブロック図。

【図6】前記照合サーバの動作を説明するためのフローチャート。

【図7】特徴データを抽出するための従来の光学方法における処理と、前記第1の実施の形態における電極アレイ方法の処理を比較するフローチャート。

【図8】光学式の一次元射影検出装置を前記第1の実施の形態に適用する場合を説明するための図。

【図9】前記第1の実施の形態に係るコンピュータネットワークシステムの変形例を示す図。

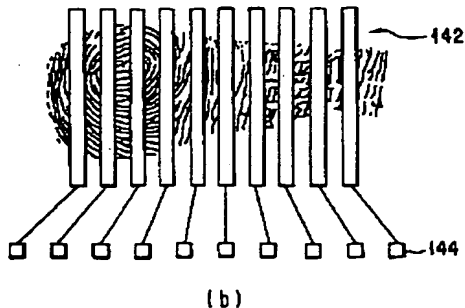
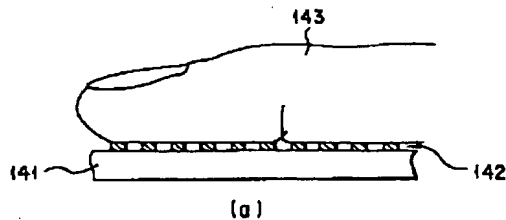
【図10】この発明の第2の実施の形態に係るワークフロー処理を説明するためのフローチャート。

【図11】この発明の第3の実施の形態に係るコンピュータネットワークシステムの概略構成を示すブロック図。

【図12】前記第3の実施の形態のコンピュータネットワークシステムにおいて、ファイルアクセス要求の生じたコンピュータシステムの処理を示すフローチャート。

【図13】前記第3の実施の形態のコンピュータネットワークシステムにおいて、他のコンピュータシステムからファイルアクセス要求を受けたコンピュータシステムの処理を示すフローチャート。

【図2】



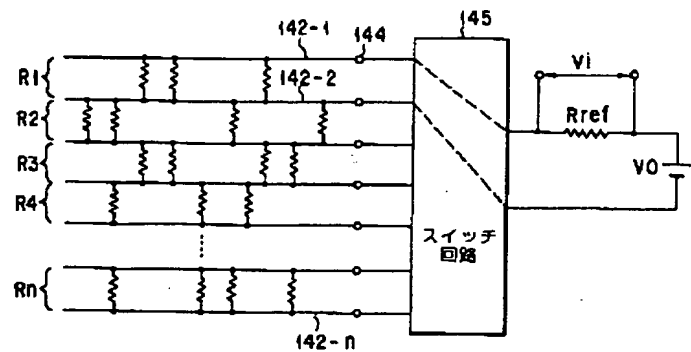
【図14】この発明の第4の実施の形態に係るコンピュータネットワークシステムの概略構成を示すブロック図。

【図15】前記第4の実施の形態のコンピュータネットワークシステムにおけるコンピュータシステム及び照合サーバの処理を示すフローチャート。

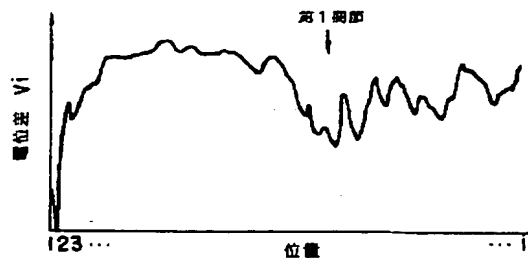
【符号の説明】

10, 20, 30, 40…コンピュータネットワークシステム、11 (11-1~11-3), 21 (21-1~21-3), 31 (31-1内31-3), 41 (41-1~41-3)…コンピュータシステム、12, 22, 32, 42…通信網、13 (13-1~13-3), 33 (33-1~33-3), 43 (43-1~43-3)…データ縮退ユニット、14 (14-1~14-3), 34 (34-1~34-3), 44 (44-1~44-3)…特徴計測ユニット、15, 25, 45…照合サーバ、16, 26, 35 (35-1~35-3), 46, 47 (47-1~47-3)…ファイルシステム、27 (27-1~27-3)…指の特徴抽出部、51…光学式指紋画像測定器、52…一次元射影計算部、53…フィルタリング・A/D変換、141…基板、142…線状電極アレイ、143…指、144…端子、145…スイッチ回路、151…位置合せ処理部、152…相違度計算部、153…比較部。

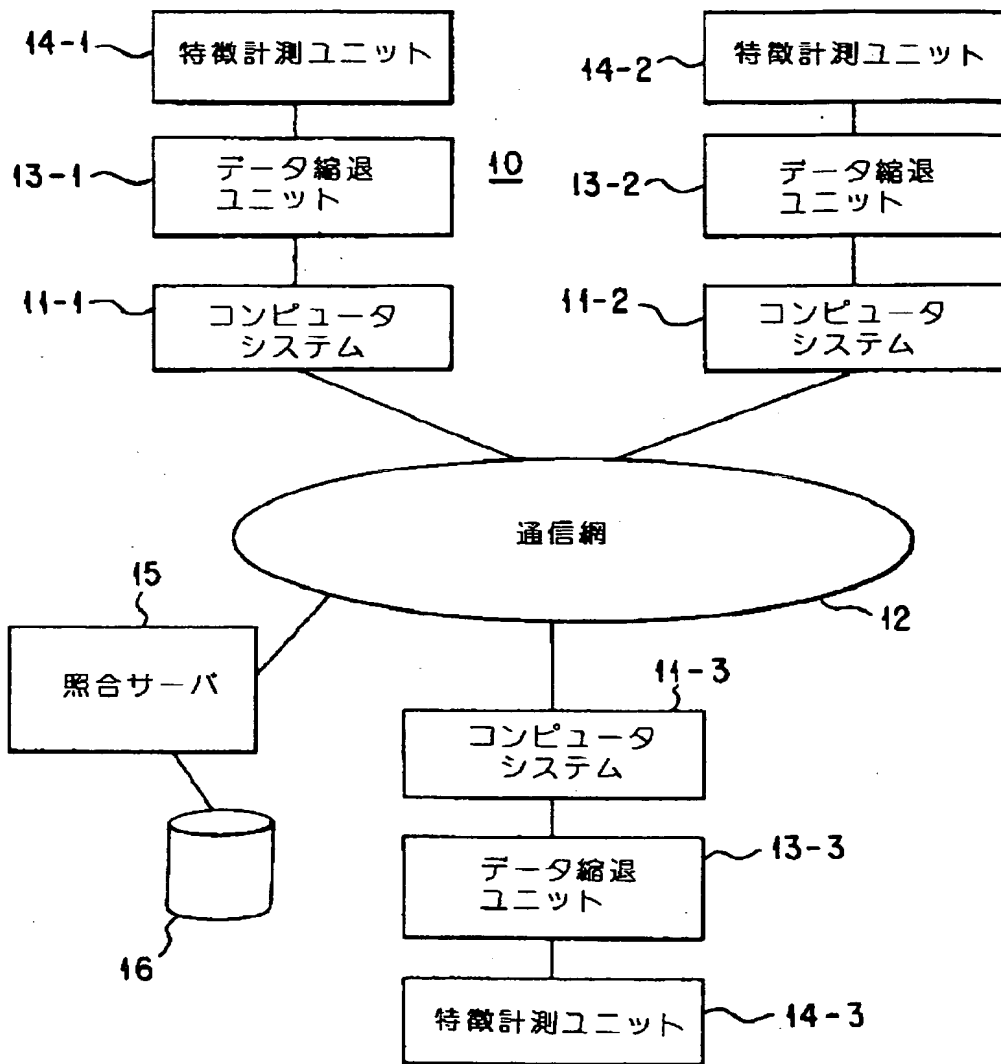
【図3】



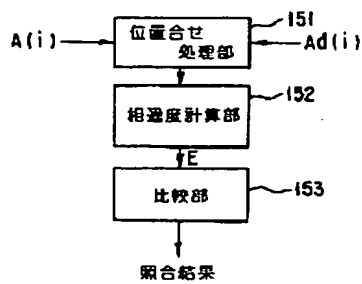
【図4】



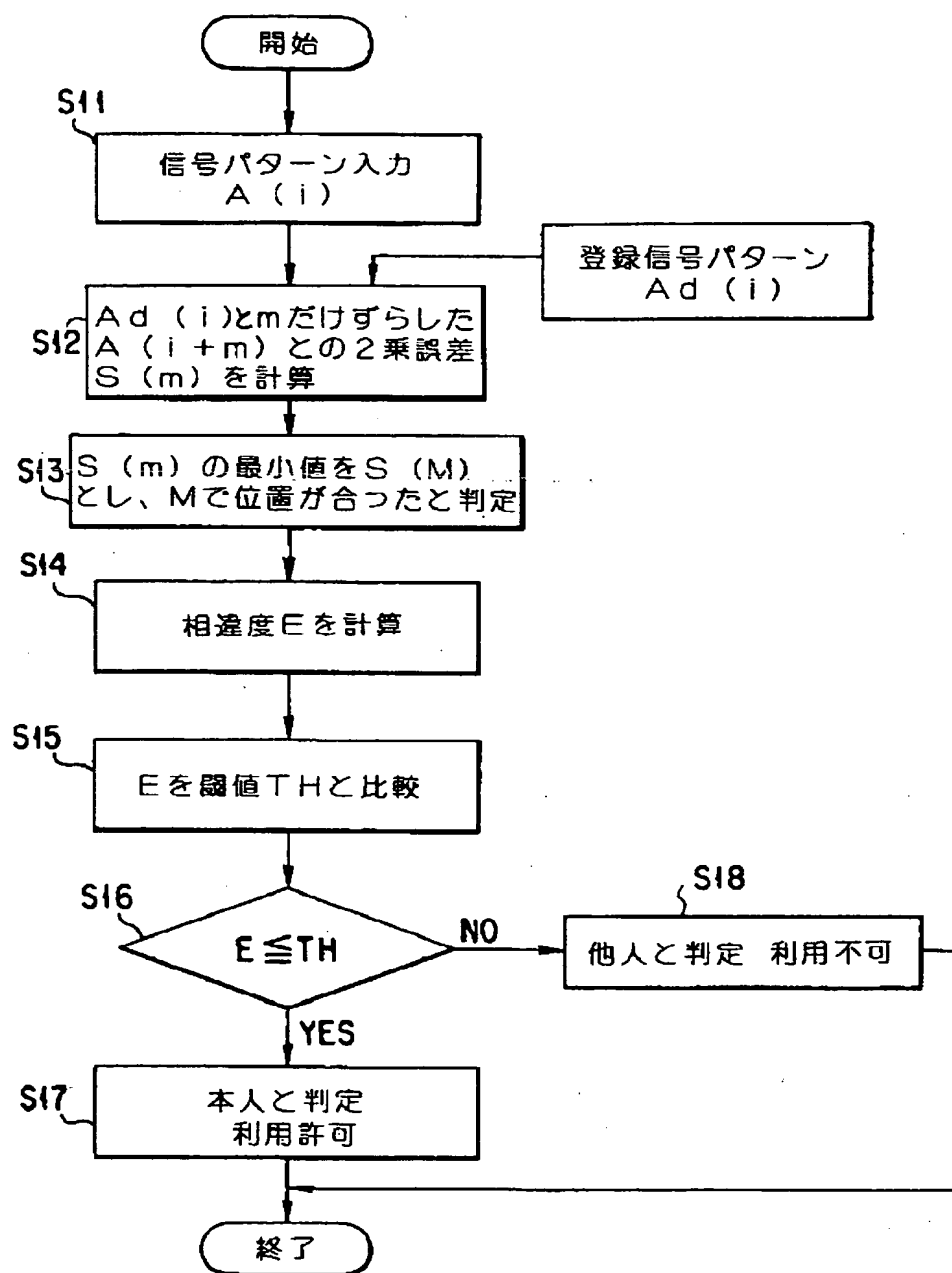
【図1】



【図5】

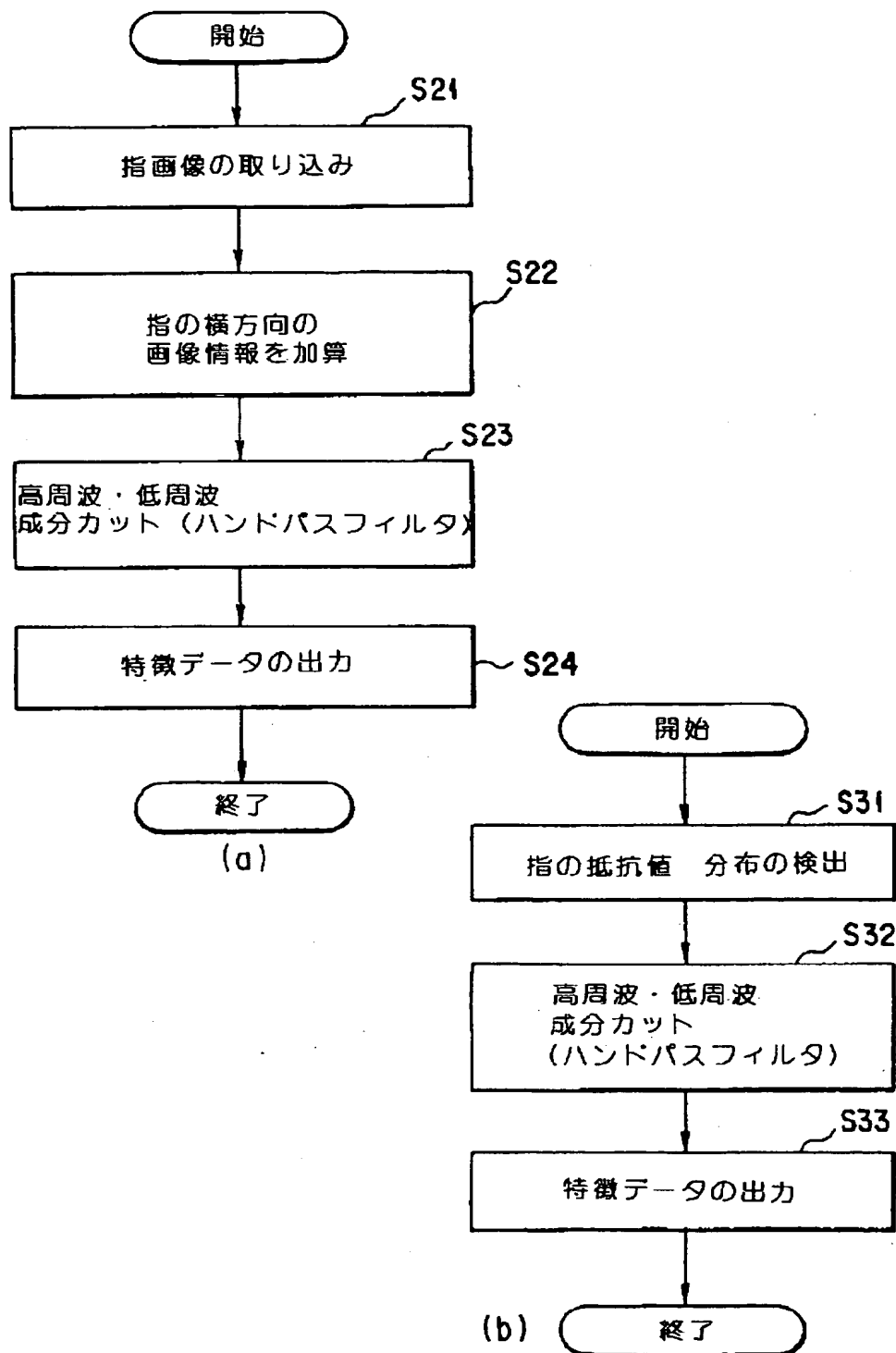


【図6】

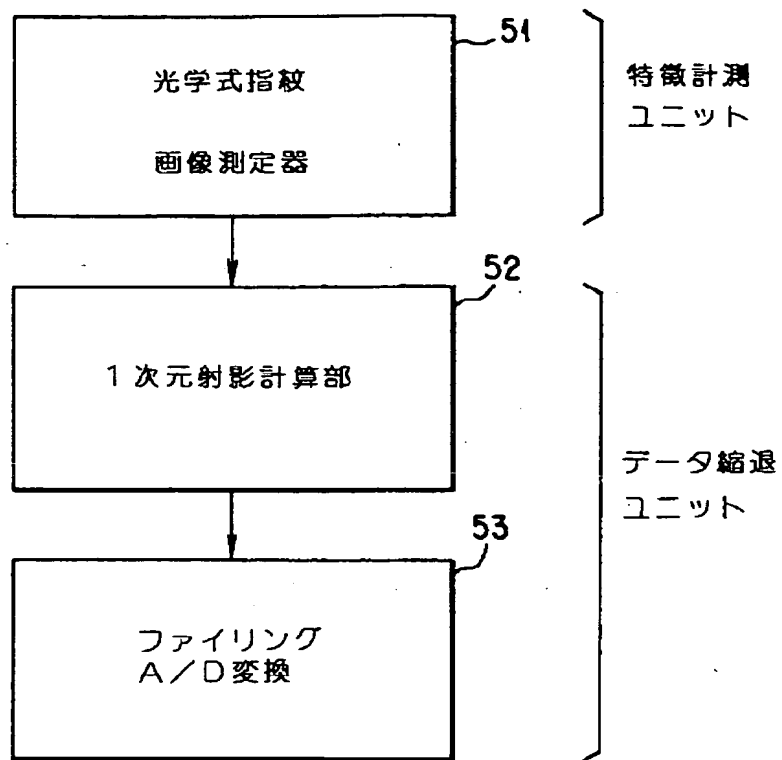




【図7】



【図8】

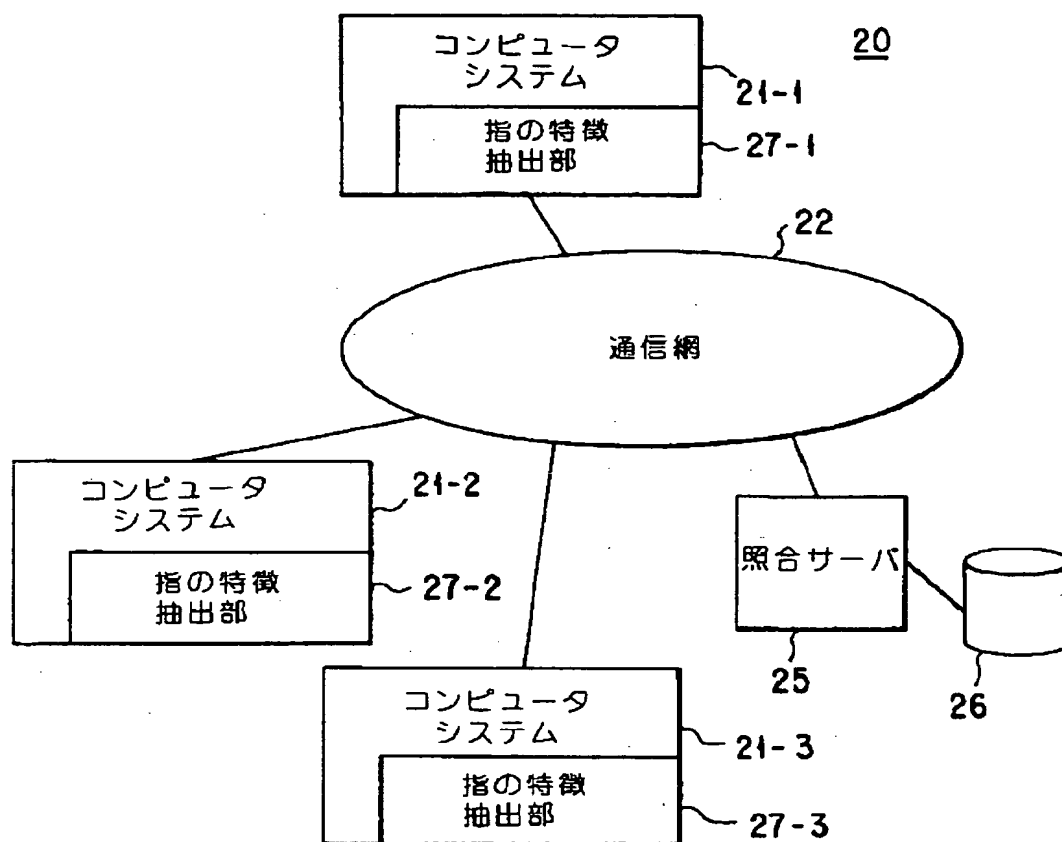


(a)

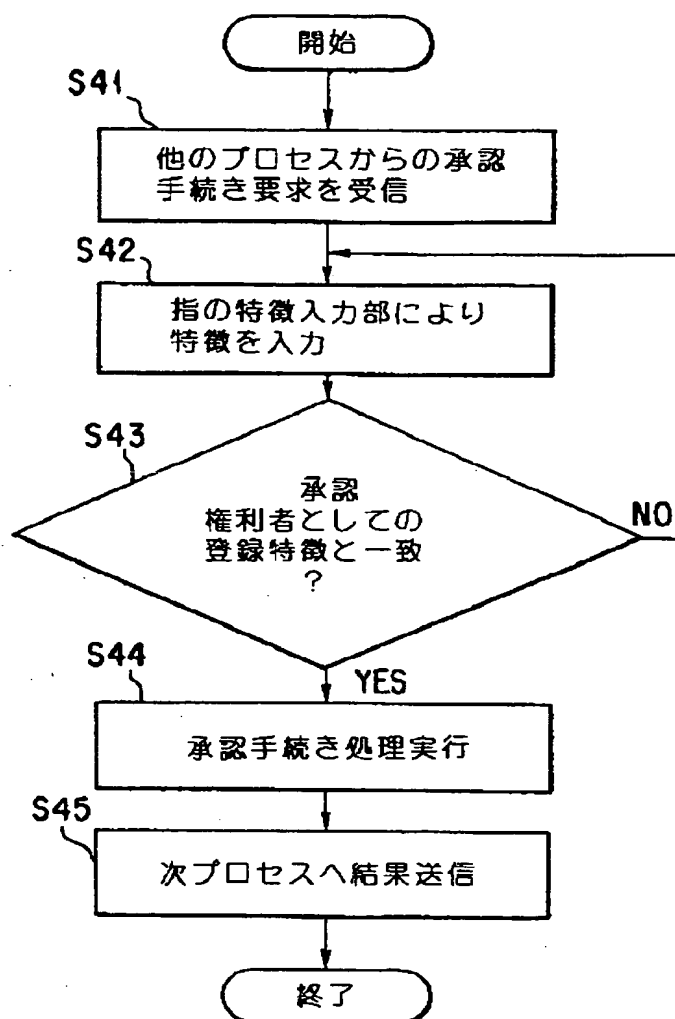


(b)

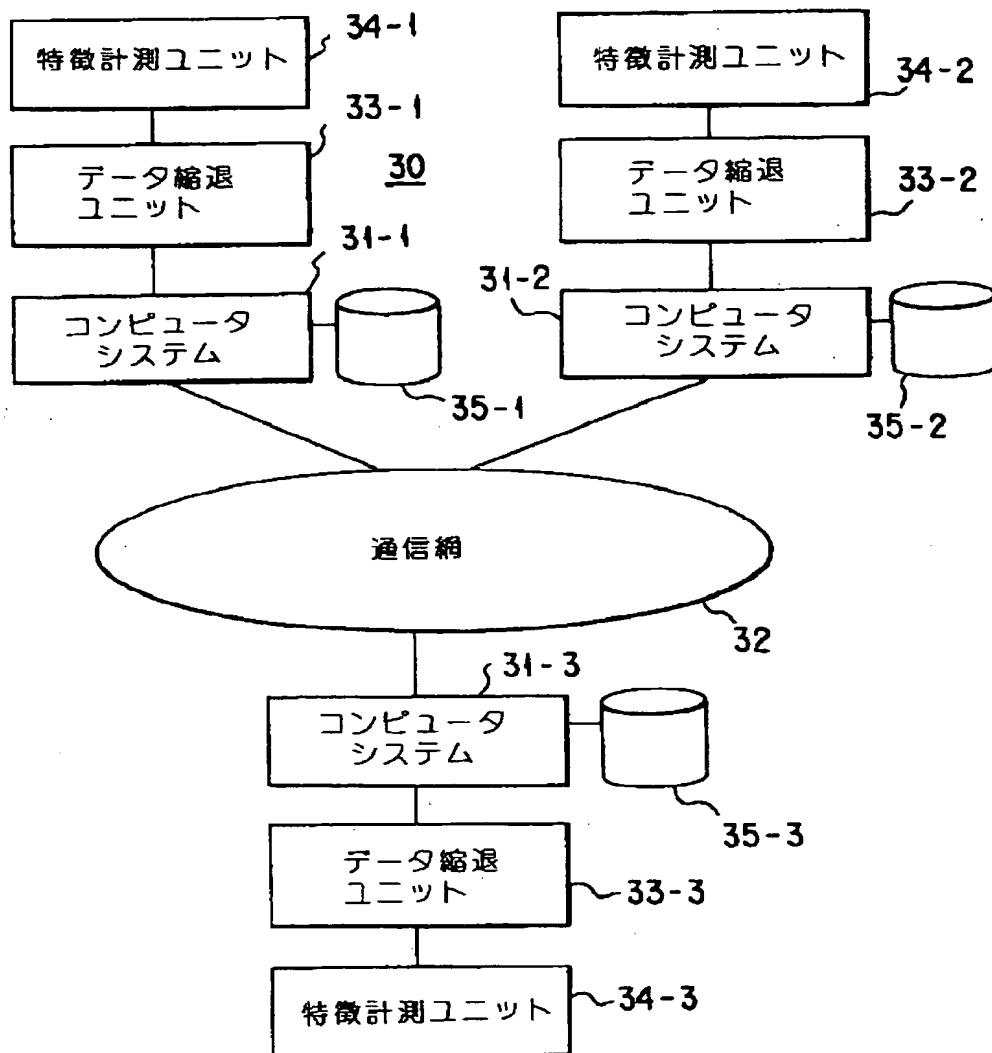
【図9】



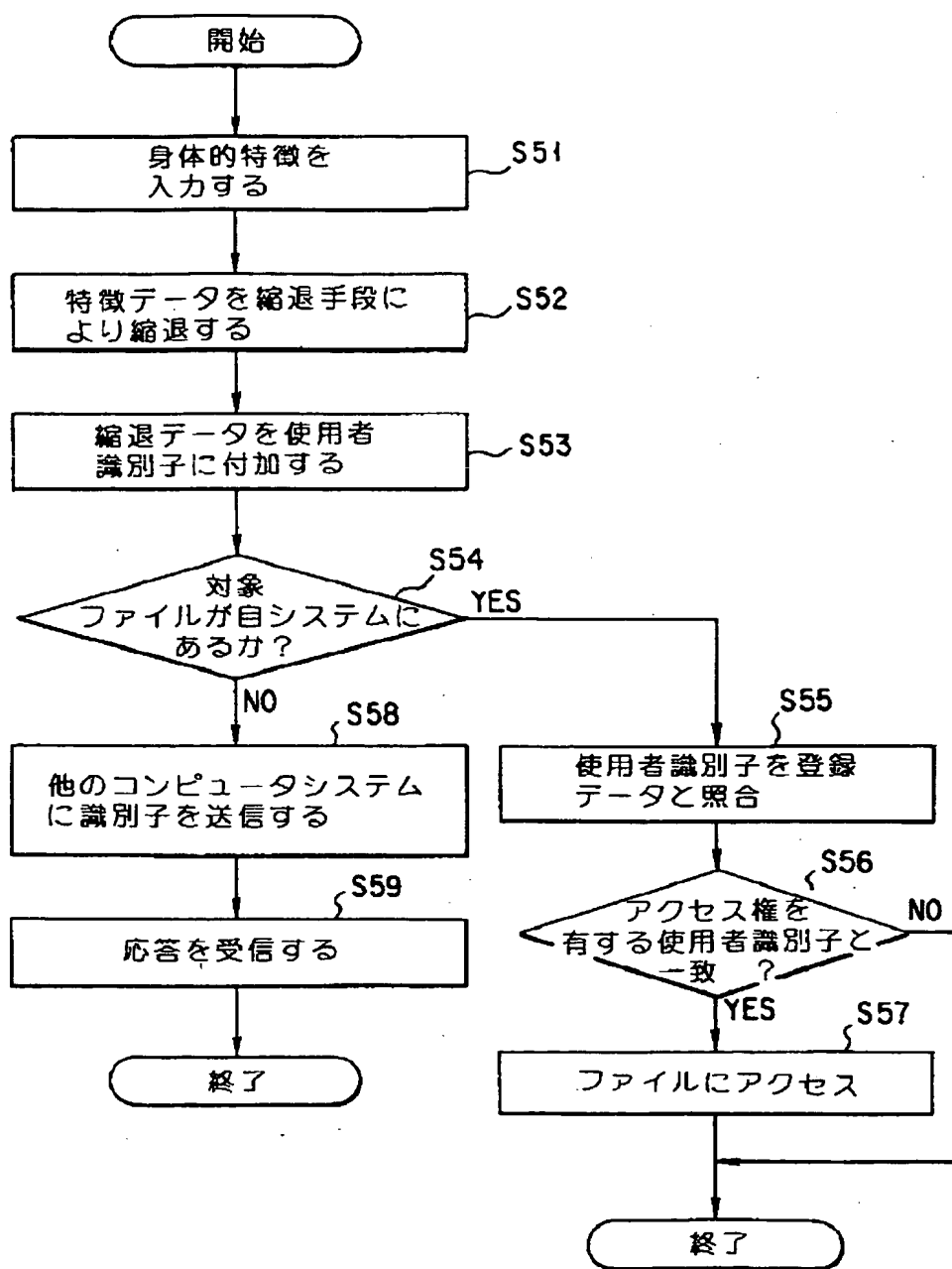
【図10】



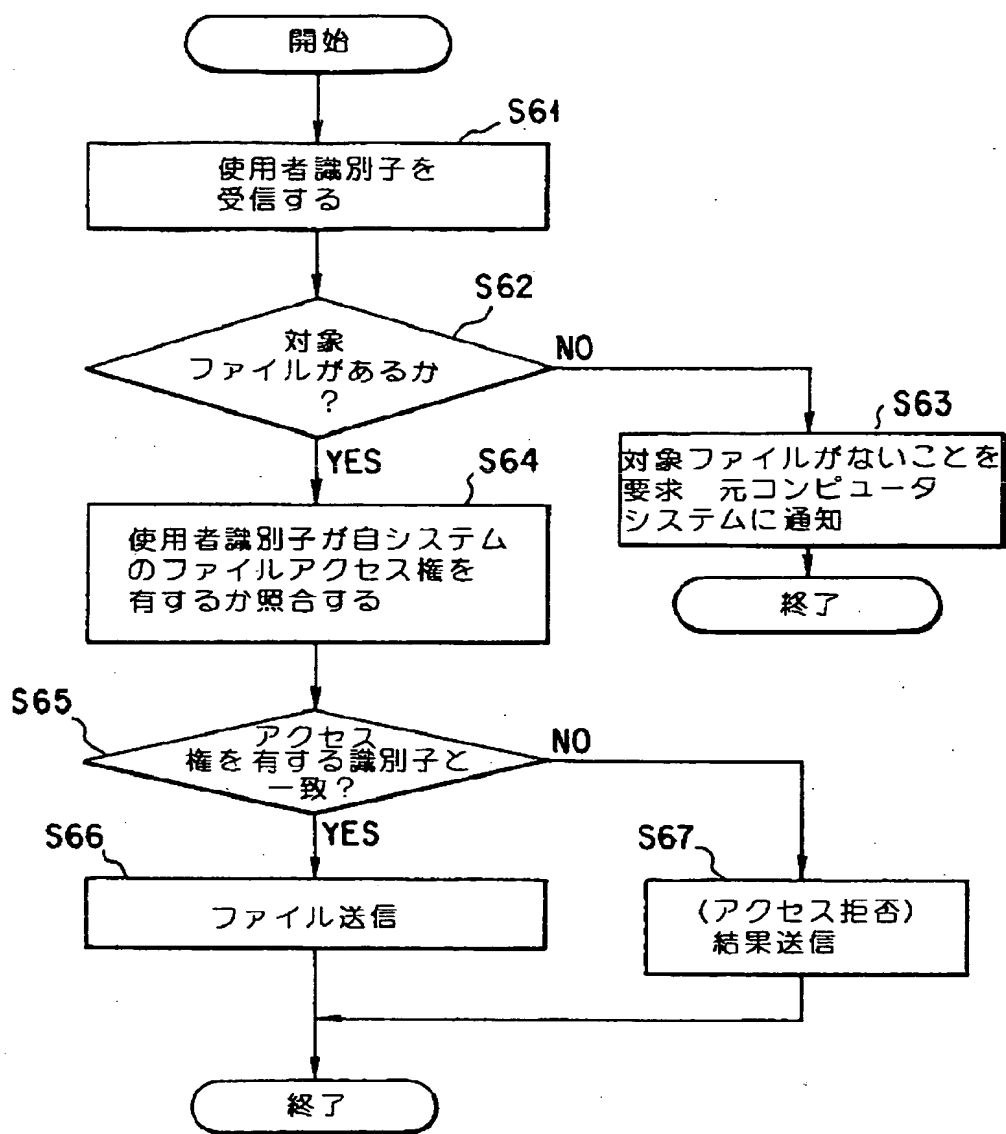
【図11】



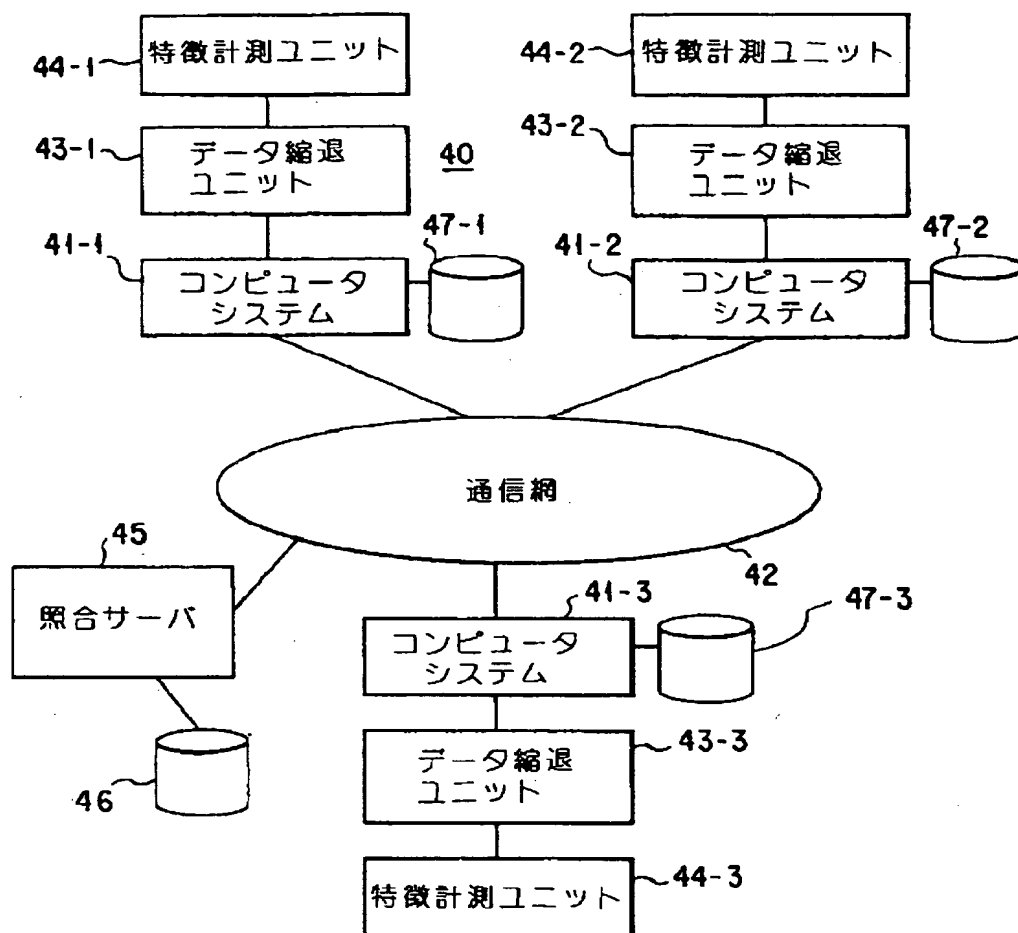
【図 12】



【図13】



【図14】





【図15】

